STEVEN M. FARINA
GEORGE A. BORDEN
MARGARET A. KEELEY
COLETTE T. CONNOR
XIAO WANG
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Tel: (202) 434-5000
Fax: (202) 434-5029
sfarina@wc.com
gborden@wc.com
mkeeley@wc.com
cconnor@wc.com
xwang@wc.com

JOHN W. SPIEGEL
(State Bar No. 78935)
ROBERT L. DELL ANGELO
(State Bar No. 160409)
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, 50th Floor
Los Angeles, CA 90071
Tel: (213) 683-9100
Fax: (213) 683-5141
john.spiegel@mto.com
robert.dellangelo@mto.com

Attorneys for Defendants Intel Corporation, Brian M. Krzanich, Robert H. Swan, and Navin Shenoy

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

IN RE INTEL CORPORATION SECURITIES LITIGATION

Case No. 4:18-CV-00507-YGR

DEFENDANTS' NOTICE OF MOTION AND MOTION TO DISMISS CONSOLIDATED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

Date:	November 13, 2018
Time:	2:00 P.M.
Courtroom:	1, 4th Floor
Judge:	Hon. Yvonne G. Rogers

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

NOTICE OF MOTION AND MOTION

TO THE COURT, ALL PARTIES, AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on November 13, 2018, at 2:00 P.M., or as soon thereafter as this matter may be heard, in Courtroom 1, 4th Floor, of this Court, located at 1301 Clay Street, Oakland, California, Defendants Intel Corporation, Brian M. Krzanich, Robert H. Swan, and Navin Shenoy (collectively, "Defendants") will and hereby do move the Court for an order dismissing with prejudice Plaintiff's Consolidated Complaint, pursuant to Federal Rules of Civil Procedure 8(a), 9(b), and 12(b)(6), and the Private Securities Litigation Reform Act of 1995.

This Motion is based upon this Notice, the accompanying Memorandum of Points and Authorities, the accompanying Request for Consideration of Documents Incorporated into Consolidated Complaint and for Judicial Notice in Support of Motion to Dismiss Consolidated Complaint, any reply memorandum, the pleadings and files in this action, and such other matters as may be presented at or before the hearing.

ISSUES TO BE DECIDED

1. Whether Plaintiff's claim under Section 10(b) of the Securities Exchange Act of 1934 should be dismissed because the Consolidated Complaint fails adequately to plead that any Defendant made any materially false or misleading statements or failed to disclose material information they had a duty to disclose.

2. Whether Plaintiff's claim under Section 10(b) should be dismissed because the Consolidated Complaint fails to allege facts giving rise to a strong inference that any Defendant acted with scienter.

3. Whether Plaintiff's control-person claim under Section 20(a) of the Exchange Act should be dismissed because the Consolidated Complaint fails adequately to plead (1) an underlying Section 10(b) claim; and (2) facts establishing the element of control as to Defendant Shenoy.

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Security vulnerabilities with technology products are ubiquitous, and thousands of new vulnerabilities are normally identified every year. In June 2017, Intel and other semiconductor

companies learned of sophisticated new methods to exploit vulnerabilities in chips made by all major manufacturers. As is normal, Intel and the industry immediately began work to develop protective countermeasures to address these vulnerabilities (which came to be known as Spectre and Meltdown). Intel and other companies followed a widely-accepted and well-known protocol known as "Responsible Disclosure," and they made no immediate public statements about the vulnerabilities because doing so before solutions were deployed would have increased the risk that malicious actors could exploit the vulnerabilities.

What is not normal about the facts of this case is that, in early January 2018, just days before the industry had planned a coordinated announcement of the solutions, news of the vulnerabilities leaked. These leaks spawned inaccurate media reports about the vulnerabilities, including that the problem could not be fixed and was unique to Intel's products. Intel's share price declined. However, accurate information soon became available and solutions were deployed. Intel's stock price quickly increased, going on to become the single best performing stock in the Dow Jones Industrial Average for the first quarter of 2018. No malicious exploitation of the vulnerabilities has ever been reported to Intel, which has announced record revenue in back-to-back quarters. Plaintiff notably has not alleged and cannot allege that Intel has suffered ***any*** material financial impact related to the issues.

Plaintiff's case rests on the fleeting stock decline and a bogus theory that Intel supposedly committed securities fraud by following established industry norms and failing to tell the world, including potential hackers, about the vulnerabilities ***before*** solutions were in place.

Plaintiff's claims fail as a matter of law, for multiple independent reasons:

First, Intel made no false or misleading statements about Spectre and Meltdown. Nor did Intel promise that its chips were generally impervious to any and all security vulnerabilities. To the contrary, Intel warned of the risks of vulnerabilities, including by stating that "no computer system can be absolutely secure." Plaintiff is relegated to arguing that Intel assumed a duty to prematurely disclose the vulnerabilities because its general marketing statements and its advertising of security features were purportedly misleading in the absence of additional information. That claim fails because the cited statements were not false or misleading, and most were the sort of vague, optimistic marketing statements that are immaterial to investors as a matter of law.

Intel had no duty to disclose the vulnerabilities for the additional reason that they were immaterial. Intel stated during the putative class period that it expected no material financial impact from the vulnerabilities, and none has emerged. In stark contrast to most other securities fraud cases, Intel has suffered no adverse financial consequences. Plaintiff has not alleged and cannot allege that Intel has taken any charge to earnings, realized any drop in revenue, or accrued any loss-contingency reserve due to these issues. Nor can the very brief dip in the stock price establish materiality under settled Ninth Circuit law. *See Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1277 (9th Cir. 2017). Indeed, the rapid and complete recovery of Intel's stock negates any inference that the vulnerabilities were material to investors.

Second, Plaintiff fails to allege specific facts giving rise to a strong inference of scienter, as is required to state a claim under the stringent standards of the Private Securities Litigation Reform Act. Any inference of fraud must be at least as compelling as inferences of innocence, and here the much more plausible inference from the facts alleged is that Intel appropriately adhered to the industry-wide Responsible Disclosure protocol—as did Microsoft, Apple, Google, Amazon, Dell, and the many other technology companies involved in deploying the solutions—and it correctly anticipated that the vulnerabilities would be remediated successfully. This case falls under the Ninth Circuit's decision in *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046 (9th Cir. 2014), which held that delaying disclosure while a company investigated problems with its chips did not give rise to a strong inference of scienter. That Intel's former CEO sold stock during the putative class period does not establish scienter because many factors militate strongly against such an inference—including that the former CEO would have profited if he had held rather than sold.

Third, Plaintiff's attempt to state a claim for control-person liability fails because it has not alleged a viable underlying violation and, as to Defendant Shenoy, the allegations of control are mere boilerplate and worthy of no credit under governing case law.

For all these reasons, the Consolidated Complaint should be dismissed.

BACKGROUND[1]

The Spectre and Meltdown Security Vulnerabilities

On June 1, 2017, a researcher working at Google on a team called Project Zero ("GPZ") notified Intel and two other microprocessor companies (AMD and Arm) that he had discovered a potential method to access information in a computer system; this vulnerability eventually became known as Spectre. ECF No. 57 (Consolidated Class Action Complaint ("CC")) ¶¶ 3, 52.[2] Later in June, GPZ identified a second, related vulnerability, which is now known as Meltdown. CC ¶ 54. These vulnerabilities could allow a hacker, using a type of attack known as a "side channel attack," to exploit a processor's use of a feature known as "speculative execution." CC ¶¶ 52, 54, 56. Processor chips have incorporated this feature, which improves processor speed, since at least the mid-1990s. CC ¶¶ 35, 39. Although speculative execution has been a feature of processors made by all major manufacturers for decades, no one before had identified these vulnerabilities, and Plaintiff does not allege that there has been any malicious exploitation of them anywhere in the world.

It is entirely normal that new security vulnerabilities were identified. For example, Microsoft's Security Response Center lists on its website more than 6,000 "Critical" and "Important" Windows security vulnerabilities that were published in 2017 alone. Ex. 1. Throughout the putative class period, Intel's website (many pages of which Plaintiff cites as a basis for its allegations) included a "Product Security Center," which listed more than 70 security vulnerabilities that had been identified in Intel products and provided information about solutions and workarounds. Ex. 2. The site also described Intel's "Bug Bounty Program," which offers rewards to researchers who identify new security vulnerabilities and bring them to Intel's attention. Ex. 2.

Upon learning of Spectre and Meltdown, Intel and other chip manufacturers set to work on developing solutions. CC ¶¶ 64, 66. These efforts involved third parties because some of the

[1] The facts in this Background section are taken from the allegations of the Consolidated Complaint, assumed to be true for purposes of this motion only, and from other sources of which the Court may take judicial notice. *See* Defendants' Request for Consideration of Documents Incorporated into Consolidated Complaint and for Judicial Notice in Support of Motion to Dismiss Consolidated Complaint. Citations to "Ex. __" are to the exhibits to the Declaration of Xiao Wang.

[2] There are two forms of Spectre, referred to as Variant 1 and Variant 2.

solutions entailed installing software patches to computer operating systems (thus requiring coordination with Microsoft, Apple, and other vendors), while others required changes to microcode that resides on the processor (thus requiring coordination with manufacturers of computers that incorporate the processor chips, such as Dell and HP). CC ¶¶ 61, 62, 66, 71. Amazon and Google, as well as many other technology companies, also participated in these efforts.

Responsible Disclosure Protocol

When GPZ informed the manufacturers about these vulnerabilities, it initially imposed a 90-day deadline (i.e., until August 31, 2017) before it would publicize the issues, which it later extended until January 2018 to allow solutions to be deployed. CC ¶¶ 6, 46, 53, 65. GPZ's approach was consistent with a widely-known "established protocol" (CC ¶ 3) in the technology industry known as Responsible Disclosure (or "Coordinated Disclosure"), which provides that security vulnerabilities should not be disclosed publicly until remedies are in place.[3] Under that protocol, Intel and the other companies involved in the remediation efforts—including Microsoft, Apple, Google, Amazon, Dell, AMD, Arm, and many others—agreed to simultaneously disclose the existence of the vulnerabilities and the solutions on January 9, 2018. CC ¶ 105.

The Responsible Disclosure standards were known to investors during the putative class period, as shown by documents cited in the Consolidated Complaint. *See, e.g.*, Ex. 4 (cited in CC ¶¶ 60, 63) ("common practice" to "keep the news [of security vulnerabilities] from the public so hackers [cannot] take advantage of the flaws"); Ex. 5 (cited and quoted in CC ¶ 69) ("the custom is to give the vendor a few months to fix the problem before it goes public and bad guys have a chance to exploit it"). These principles are publicized in various forums, including the CERT® Guide to Coordinated Vulnerability Disclosure (published in August 2017).[4] The rationale is that disclosure of vulnerabilities without solutions "only opens the public up to exploitation," and that the "ideal

[3] When GPZ was established in 2014, it stated its expectation that vulnerabilities would become public "typically once a patch is available." Ex. 3.

[4] Ex. 6. The CERT Guide is published by the CERT Coordination Center ("CERT/CC"), which is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. The Consolidated Complaint refers to CERT/CC as a "trusted third party in the vulnerability coordination and disclosure process." CC ¶ 68.

scenario occurs when everyone coordinates and cooperates to protect the public." Ex. 6 at 7. Premature release of even minimal information about a vulnerability may "help adversaries" because "the mere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves." Ex. 6 at 51.

Throughout the putative class period, Intel made clear to the public that it followed the Responsible Disclosure protocol. For example, it stated that it "works to best ensure that security vulnerabilities affecting Intel production products are documented and solutions are released in a responsible fashion," and that "[v]ulnerability information is extremely sensitive." Ex. 7. It also publicly thanked researchers who identified vulnerabilities for "working with us on a coordinated disclosure." *See, e.g.*, Ex. 8.

Intel's Warnings Concerning Security Vulnerabilities

In addition to advising the public about the existence of possible security vulnerabilities and the manner in which they would be disclosed, Intel warned investors of the associated risks. In its 2016 10-K filed in February 2017, Intel stated:

> **[M]alicious hackers** may attempt to gain **unauthorized access** and corrupt **the processes of hardware and software products that we manufacture** . . . . [O]ur products . . . are **a frequent target** of computer hackers and organizations that intend to sabotage, take control of, or otherwise corrupt our . . . products . . . . We believe such attempts are increasing in number and in technical sophistication. **From time to time, we encounter intrusions or unauthorized access to our . . . products** . . . . [W]e remain **potentially vulnerable** to additional **known or unknown threats**. Such incidents, whether successful or unsuccessful, could result in our incurring significant costs related to, for example, . . . providing **modifications to our products** . . . , defending against litigation, responding to regulatory inquiries or actions, paying damages, or **taking other remedial steps** with respect to third parties. Ex. 9 (emphasis added).

Public Disclosure of the Vulnerabilities

After a series of leaks, on January 2, 2018, a technology publication called The Register published an article about the vulnerability now known as Meltdown. CC ¶ 105. Both variants of Spectre also soon became public. CC ¶ 108.

After the close of trading on January 3, Intel made its first public statement about the

vulnerabilities. CC ¶ 107. Intel stated that it "is committed to the industry best practice of responsible disclosure of potential security issues, which is why Intel and other vendors had planned to disclose this issue next week when more software and firmware updates will be available," but that Intel was speaking out now to correct "current inaccurate media reports." Ex. 10. Intel first corrected reports that the vulnerabilities only affected Intel's products.[5] Intel also stated that it had begun providing software and firmware (microcode) updates to remediate the vulnerabilities, correcting reports that the vulnerabilities had no solutions.[6]

Also on the evening of January 3, Intel convened an analyst conference call to further explain Spectre and Meltdown. CC ¶¶ 110, 111. Among other things, Intel's representatives stated that "we really don't anticipate any material impact to our business"; that the remediation imposed "no meaningful cost" on Intel; and that "we do not expect any financial implication" from the vulnerabilities. Ex. 12. They also explained that although Intel viewed its solutions as effective, it "will be pursuing hardware initiatives or hardware improvements for both performance and security going forward," CC ¶ 111, and that "as we make changes in the hardware, you should expect to see that the impact of those mitigations have a lower performance impact than the mitigations that we're using today for products in the field." Ex. 12.

[5] For example, The Register article, quoted in Consolidated Complaint paragraph 105, stated that AMD, Intel's competitor, "says it is not affected," presumably because AMD maintains that it is not affected by Meltdown—even though its products are subject to both variants of Spectre. Not until January 11 did AMD release a statement clarifying that its chips are susceptible to Spectre Variant 2 (as well as Variant 1). AMD investors are now suing AMD, alleging that the January 11 announcement was the revelation of the truth concealed by AMD's earlier statement that its products had "near zero risk" of Spectre Variant 2. *See* Am. Class Action Compl. for Violation of the Fed. Sec. Laws, *Kim v. Advanced Micro Devices, Inc.*, No. 5:18-cv-00321-EJD, ECF No. 36 (N.D. Cal. Aug. 3, 2018).

[6] Examples of these inaccurate statements included a New York Times article cited in Consolidated Complaint paragraph 63, which reported that there was "no known fix" for Spectre, and a CERT/CC publication referred to in paragraph 69, which incorrectly stated that "[f]ully removing the vulnerability requires replacing vulnerable CPU hardware." Exs. 4 & 5. Plaintiff cites the incorrect CERT/CC statement (CC ¶ 59 & n.14) and alleges that CPU replacement is necessary, but fails to acknowledge that "[o]ne day after recommending that the only way to address the security issue was to replace the CPU, CERT/CC . . . dropped that recommendation entirely" and instead advised installing software updates. Ex. 11.

Post-Class Period Events

On January 25, 2018, Intel announced its financial results for the fourth quarter of 2017. Ex. 13. Intel's earnings release showed again that the company did not suffer any material financial impact from Spectre and Meltdown. Ex. 13. Intel announced "record fourth-quarter revenue [of] $17.1 billion and record full-year revenue [of] $62.8 billion," Ex. 13, and its stock rose to a 17-year high, closing at $50.08. Ex. 14.

Intel's stock price continued to rise throughout the first quarter of 2018. In fact, Intel was the best-performing stock in the Dow Jones Industrial Average for the first quarter, rising more than 12%. Ex. 15. The average dividend-adjusted closing price in the 90 days following the final alleged corrective disclosures was $48.19. (By comparison, the average dividend-adjusted closing price during the putative class period was $45.17.) Ex. 14. Although the Consolidated Complaint cites reports that any financial impact of Spectre and Meltdown would be felt by mid-February 2018, CC ¶ 116, on April 26, 2018, Intel announced first-quarter results showing "record first-quarter revenue [of] $16.1 billion, up 13 percent year-over-year." Ex. 16.

ARGUMENT

To state a claim under Section 10(b), a complaint must allege facts sufficient to establish (1) that the defendant made a materially false or misleading statement; (2) that the defendant did so with scienter; (3) that the statement was made in connection with the purchase or sale of a security; (4) that the plaintiff relied upon the statement; (5) economic loss; and (6) loss causation. *Loos v. Immersion Corp.*, 762 F.3d 880, 886–87 (9th Cir. 2014). Securities-fraud complaints must meet the stringent pleading standards of Federal Rule of Civil Procedure 9(b) and the Private Securities Litigation Reform Act, which requires a plaintiff to plead falsity and scienter with particularity. 15 U.S.C. § 78u-4(b)(1)-(2); *Zucco Partners LLC v. Digimarc Corp.*, 552 F.3d 981, 990–91 (9th Cir. 2009). Plaintiff's Consolidated Complaint does not come close to meeting these standards.

I. Defendants Made No False or Misleading Statements and Had No Duty To Disclose Additional Information.

To survive a motion to dismiss, a complaint must "specify each statement alleged to have been misleading [and] the reason or reasons why the statement is misleading." *Metzler Inv. GmbH v.*

Corinthian Colls., Inc., 540 F.3d 1049, 1061 (9th Cir. 2008) (internal citation and quotation marks omitted). Statements are misleading only if they "affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists." *In re Dynavax Sec. Litig.*, 2018 WL 2554472, at *5 (N.D. Cal. June 4, 2018) (internal citation and quotation marks omitted), *appeal docketed*, No. 18-16250 (9th Cir. July 6, 2018)). "Silence, absent a duty to disclose, is not misleading under Rule 10b-5." *Basic Inc. v. Levinson*, 485 U.S. 224, 239 n.17 (1988). "Thus, as long as [any] omissions do not make the actual statements misleading, a company is not required to disclose" other facts "even if investors would consider the omitted information significant." *In re Rigel Pharm., Inc. Sec. Litig.*, 697 F.3d 869, 880 n.8 (9th Cir. 2012).

Moreover, vague, optimistic statements are not actionable because they do not induce reliance by reasonable investors and thus are immaterial as a matter of law. *See Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 606 (9th Cir. 2014); *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d 1051, 1060 (9th Cir. 2014); *In re Cutera Sec. Litig.*, 610 F.3d 1103, 1111 (9th Cir. 2010); *In re Solarcity Corp. Sec. Litig.*, 274 F. Supp. 3d 972, 995–96 (N.D. Cal. 2017). Any statement that is not "capable of objective verification" falls into this category. *Apollo*, 774 F.3d at 606.

The Consolidated Complaint falls far short under these well-accepted standards. Plaintiff pleads no legal basis for a duty of disclosure other than the contention that Intel's statements were purportedly incomplete and therefore misleading. The great majority of those statements were not even directed to investors, but rather were product advertisements on Intel's website. Such statements have little probative value in a securities case and do not satisfy the bedrock requirement that statements be made "in connection with the purchase or sale of [any] securit[y]." *Bien v. LifeLock, Inc.*, 2015 WL 12819154, at *9 (D. Ariz. July 21, 2015) (internal quotation marks omitted), *aff'd sub nom. In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x. 947 (9th Cir. 2017). Moreover, none of Defendants' statements promised that Intel's products were immune from vulnerabilities. And none created a duty to disclose Spectre and Meltdown prematurely.

A. Statements About Chip Security Were Not Materially False or Misleading.

1. Factual Statements About Chip Security Were True and Not Misleading.

Plaintiff highlights a number of statements Defendants made about the security benefits of

Intel's products. Most were immaterial as a matter of law (*see* Section I.A.2 *infra*). To the extent Defendants' chip-security statements included specific factual content, they addressed features of Intel products that enhance data security. These include Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI); Intel® Online Connect; Intel® Authenticate Solution; Intel® Software Guard Extensions (Intel® SGX); Intel® BIOS Guard; Intel® Boot Guard; Intel Active Management Technology (Intel AMT); Intel® vPro™ platform; Intel® Platform Trust Technology; Execute Disable Bit; Advanced Encryption Standards (AES); and Secure Hash Algorithm (SHA). CC ¶¶ 132–52. Plaintiff pleads no facts showing that these features are absent from Intel products, or that they fail to provide security-related benefits.[7]

Notably, none of these statements promised that Intel's products were impervious to any and all security vulnerabilities, let alone promise immunity to side-channel attacks generally or to Spectre and Meltdown specifically. Nor could they reasonably be interpreted to suggest this. In fact, many of the web pages Plaintiff cites include an express warning that "[n]o computer system can be absolutely secure."[8] Generally, they conveyed only that the features in question "strengthen[ed]" or "improved" security, thereby "reducing [users'] exposure" to attacks (CC ¶¶ 138, 140, 144, 152)—not eliminating that exposure.

No reasonable investor learning of these features could have been misled to believe that Intel's chips are immune from all forms of attack. *See Dynavax*, 2018 WL 2554472, at *6 (company statements "cannot reasonably be said to have misled investors into believing that no cardiac adverse events had occurred"). The risk that computers can be hacked is common knowledge. Especially in light of the market's awareness of (a) the ubiquity of security vulnerabilities (including at Intel), (b)

[7] Indeed, the highlighted security features reduce the risk of many common forms of cybercrime. For example, some of the advertised technologies enable data encryption, so that online shoppers can provide credit card information more safely even if a bad actor intercepts the communication. Others enable identity-authentication methods such as fingerprint recognition, which help guard against theft of data or introduction of malicious code by actors who gain physical access to a user's computer. CC ¶¶ 132, 136, 140.

[8] *See, e.g.*, Ex. 17 (examples of this disclaimer as it appeared on Intel's "Xeon® E3 Processors" product web page (cited at CC ¶ 148) during the putative class period and as it appeared on Intel's "Pentium® and Celeron® Processors" product web page (cited at CC ¶ 152) even before the putative class period).

Intel's warnings that its products are a "frequent target of computer hackers" and "remain vulnerable," (c) Intel's adherence to Responsible Disclosure, and (d) its express disclaimer that no computer system can be absolutely secure, any reasonable investor would have realized that security vulnerabilities like Spectre and Meltdown were possible, and that Intel might be working on addressing such issues at any given time. Stated differently, nothing about Intel's statements was "necessarily inconsistent" with the actual facts. *In re Read-Rite Corp.*, 335 F.3d 843, 846–48 (9th Cir. 2003), *abrogated on other grounds as recognized in South Ferry LP, No .2 v. Killinger*, 542 F.3d 776, 782–84 (9th Cir. 2008).

Plaintiff's allegations that Defendants misled investors by "concealing that the only permanent solution to address Spectre and Meltdown was a fundamental redesign" of Intel's chips (CC ¶ 141) is a non-starter. For the majority of the putative class period, Intel said nothing about Spectre and Meltdown and thus could not have misled anyone about the solutions to those issues. In addition, its cybersecurity warnings alerted investors to the possibility that security vulnerabilities, even if not successfully exploited, could require "modifications to our products." Ex. 9. The allegedly corrective disclosure quoted by Plaintiff—the statement by Intel on January 3 that it intends to "pursu[e] hardware initiatives or hardware improvements for both performance and security going forward" (CC ¶ 111)—in no way establishes that any of Intel's marketing statements were misleading, since none of those statements promised perfect and permanent protection. Nor did the January 3 statement mean that the immediate solutions are "ineffective." To the contrary, the Intel representative stated that the main benefit of future hardware improvements would be to "lessen the [performance] impact." CC ¶ 111. In any event, Plaintiff pleads no facts suggesting that the deployed solutions have failed to accomplish their objective of preventing data theft through exploitation of Spectre and Meltdown.

The holding of *LifeLock* is instructive. There, a company selling an identify-theft protection service stated: "We ensure that our systems are free from critical vulnerabilities by conducting regular vulnerability scans and penetration tests"; "we conduct internal security testing to ensure current practices are effective against emerging threats"; "we offer notifications and alerts, including proactive near real-time, actionable alerts that provide members peace of mind"; and that its service

"helps proactively safeguard your credit, your finances and your good name with vigilant services that alert you of potential threats before the damage is done." *Bien*, 2015 WL 12819154, at *6, *8.[9] The district court held, and the Ninth Circuit agreed, that these statements were not actionable despite allegedly undisclosed problems. The Ninth Circuit noted that none of the company's statements "promis[ed] perfect service," and it found the statements not false or misleading. *LifeLock*, 690 F. App'x. at 953. The same conclusion applies here.

2. Most of the Chip-Security Statements Were Immaterial as a Matter of Law.

The great majority of the chip-security statements Plaintiff cites were marketing statements to the effect that Intel's products offer security-related features that, for example, are "rock-solid" (CC ¶ 132); provide a "critical foundation for secure IT" (CC ¶ 136); and thus allow computer users to have "peace of mind" (CC ¶¶ 138, 152).[10] None of these statements was a verifiable statement of fact. They were instead the sort of vague positive statements that courts deem immaterial as a matter of law. *See, e.g.*, *Kelly v. Elec. Arts, Inc.*, 2015 WL 1967233, at *7–8 (N.D. Cal. Apr. 30, 2015) ("de-risked" technology, like the word "improved," "signifies making a product better or safer, and is a statement of corporate optimism and a vague assessment of past results"); *In re Cisco Sys. Inc. Sec. Litig.*, 2013 WL 1402788, at *13 (N.D. Cal. Mar. 29, 2013) ("strong foundation"); *Shemian v. Research In Motion Ltd.*, 2013 WL 1285779, at *6, *20–23 (S.D.N.Y. Mar. 29, 2013) ("advanced security features"), *aff'd*, 570 F. App'x. 32 (2d Cir. 2014); *Wozniak v. Align Tech., Inc.*, 850 F. Supp. 2d 1029, 1036 (N.D. Cal. 2012) ("trusted advisor"; "improved features"); *Brodsky v. Yahoo! Inc.*, 592 F. Supp. 2d 1192, 1200 (N.D. Cal. 2008) ("on the technology front we hit the ball out of the park";

[9] *See also Bien*, ECF No. 75 (Second Consolidated Amended Class Action Complaint for Violations of Federal Securities Laws) (Jan. 16, 2015).

[10] All the other chip-security statements cited by Plaintiff were equally or more vague. *See* CC ¶¶ 88 ("optimized . . . for data protection"); 134 ("protected internet and email content"); 140 ("Built-in protection runs deeper than just software."); 142 ("optimal data security"); 144 ("count on hardware-based security"); 146 ("critical foundation for secure IT"); 148 ("hardware-enhanced security"); 150 ("more robust, vulnerability-resistant platform"); 152 ("Security you can trust"; "more secure operating environment"); 160 ("designed to optimize not only performance but security"); 162 ("all the CIOs, are dealing with . . . more cybersecurity threats").

"attractive advertising platform"); *In re LeapFrog Enters., Inc. Sec. Litig.*, 527 F. Supp. 2d 1033, 1049–50 (N.D. Cal. 2007) ("consumers love our service"; demand "more vibrant than ever"); *In re Managed Care Litig.*, 150 F. Supp. 2d 1330, 1346 (S.D. Fla. 2001) ("Rock Solid health coverage").

B. Statements About Chip Performance Were Not Materially False or Misleading.

1. Factual Statements About Performance Were True and Not Misleading.

As with the chip-security statements, most of the performance-related statements listed in the Consolidated Complaint are vaguely optimistic statements that are immaterial as a matter of law (*see* Section I.B.2 *infra*). A few of Defendants' statements about chip performance were arguably specific enough to be verifiable, but Plaintiff pleads no facts showing that these statements were false or misleading. In particular, the Consolidated Complaint quotes the following statements:

- Intel Pentium and Celeron processors have "30% more processor performance and 45% better graphics on Windows than the previous generation platform" (CC ¶ 152);
- Intel's Coffee Lake family of processors has "up to 50% better performance than the competition on top-game titles" (CC ¶¶ 91, 155);
- Intel Xeon Scalable Processors have a "1.73X average performance boost vs. the previous generation across key industry-standard workloads," and "are optimized to deliver 2.2X higher deep learning training and up to 2.4X higher inference performance compared to the prior generation" (CC ¶¶ 93, 157);
- Intel Xeon Scalable Processors "outperform[] [other x86 products in the marketplace] on throughputs, kind of benchmarks by 34%, by 18% on performance per watt benchmarks and by over 50% on performance per core" (CC ¶¶ 97, 159–60); and
- Intel's Core products from 2014 to the present have "seen an over 30% improvement in the performance of the devices" (CC ¶ 165).

The Consolidated Complaint sets forth no facts showing that these statements were untrue, nor any basis to believe that they later became misleading because of the solutions deployed for Spectre and Meltdown. Most of the statements compare newer to older products, but as the Consolidated Complaint expressly acknowledges, "Spectre and Meltdown affect nearly every processor Intel has released since 1995," CC ¶ 3, so the remediation would apply to both the newer and older products

being compared.[11] *See Wochos v. Tesla, Inc.*, 2018 WL 4076437, at *7 (N.D. Cal. Aug. 27, 2018) (finding statement that "We've got I think a much better supply chain in place" for new car model compared to prior models not actionable where plaintiffs did "not put forth any facts tending to show that this was not the case"). Similarly, Plaintiff pleads no facts showing that comparisons to competitors' products are inaccurate, especially since the Consolidated Complaint acknowledges that the vulnerabilities also affect the products of Intel's competitors (CC ¶ 51).

Absent a viable allegation that any of Defendants' statements misled investors, Plaintiff's assertion that Intel had a duty to disclose Spectre and Meltdown earlier fails at the threshold. *See, e.g.*, *Rigel*, 697 F.3d at 880 n.8. So, too, does the allegation that Intel "concealed" the fact that the solutions could have a performance impact. Intel said nothing during the putative class period that created any duty for it to reveal that alleged fact, when it was adhering to the Responsible Disclosure protocol as to the vulnerabilities themselves.

2. The Performance Statements Were Immaterial as a Matter of Law.

Other than the statements discussed above, all of the performance-related statements addressed in the Consolidated Complaint are immaterial as a matter of law. These statements speak of "a big jump in performance"; "exceptional . . . performance"; "amazingly responsive systems"; "focus on speed"; "essential performance"; "professional-grade compute performance"; "significant performance improvement"; and "outstanding performance." CC ¶¶ 132, 136, 138, 142, 144, 148, 154, 160. None of these statements is objectively verifiable, and they are therefore immaterial. They all fall easily within the legion of cases that hold such statements not actionable. *See, e.g.*, *Solarcity*, 274 F. Supp. 3d at 994–95 ("amazing quarter"; "incredibly strong sales"); *Elias v. Hewlett-Packard Co.*, 950 F. Supp. 2d 1123, 1132–34 (N.D. Cal. 2013) ("ultra-reliable performance"; "delivers the power you need"; "packed with power"); *Shemian*, 2013 WL 1285779, at *6, *20–23 ("industry leading performance"; "uncompromised web browsing"; "the world's first professional-grade tablet"); *Oestreicher v. Alienware Corp.*, 544 F. Supp. 2d 964, 973 (N.D. Cal. 2008) ("faster, more

[11] Plaintiff cites a footnote, now on Intel's website (*see, e.g.*, CC ¶ 129), stating that the solutions "may make these results inapplicable to your device or system." This general disclaimer was added after the putative class period ended and after the solutions were deployed. CC ¶ 129. It does not show that any of Defendants' statements were false during the putative class period.

powerful, and more innovative than competing machines"; "superb, uncompromising quality").

C. The Vulnerabilities Were Not Material to Investors.

An additional reason the Consolidated Complaint fails to establish a duty to disclose the Spectre and Meltdown issues is that it pleads no facts showing that this information was material to investors. To satisfy the materiality requirement, there must be "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the total mix of information made available." *Basic*, 485 U.S. at 231–32 (internal citation and quotation marks omitted). When the financial import of omitted information is *de minimis*, the omission may be deemed immaterial as a matter of law. *See In re Hansen Nat. Corp. Sec. Litig.*, 527 F. Supp. 2d 1142, 1161 (C.D. Cal. 2007).

Plaintiff alleges that Intel "concealed" that its chips were "vulnerable to hacking" by Spectre and Meltdown (*e.g.*, CC ¶¶ 133, 135, 137), yet the Consolidated Complaint—filed more than six months after the vulnerabilities leaked—fails to identify a single malicious exploitation. Nor does Plaintiff plead any facts indicating that malicious exploitation was likely as of the time of Defendants' statements—when Intel was preparing to deploy solutions—or that there would have been a material impact on Intel even if successful attacks had occurred. *See Basic*, 485 U.S. at 238–39 (materiality determination of contingent or speculative event must consider probability of event occurring and potential magnitude of event).

Plaintiff also alleges that Defendants "concealed" the effectiveness and performance impact of solutions, but those facts could be material to investors only if they impacted Intel's business. The Consolidated Complaint pleads no facts that suggest there has been any such impact. Plaintiff does not allege that Intel's revenue or earnings suffered as a result of Spectre and Meltdown, and the company's outstanding performance in the first quarter of 2018 would belie any such assertion. Nor has Plaintiff alleged any other form of material financial impact. Many cases have found omitted information to be immaterial in such circumstances, even when the financial impact was far greater. *See, e.g.*, *ECA & Local 134 IBEW Joint Pension Tr. of Chicago v. JP Morgan Chase Co.*, 553 F.3d 187, 204 (2d Cir. 2009) (accounting misclassification of $2 billion not material where company had $715 billion in assets); *In re Novatel Wireless Sec. Litig.*, 830 F. Supp. 2d 996, 1015 (S.D. Cal. 2011)

(standard measure for whether alleged improper revenue recognition was material was whether it impacted revenue by 5%).

That Intel's stock price dipped briefly does not establish that the alleged omissions were material. The Ninth Circuit has declined to adopt a rule that stock-price movement equates to materiality. *See Retail Wholesale*, 845 F.3d at 1277; *see also Intuitive Surgical*, 759 F.3d at 1060. And, in any event, Intel's stock price quickly recovered, and in fact was the top-performing stock in the Dow Jones average in the first quarter of 2018, increasing by more than 12%. A quick recovery "negates any inference of materiality, because it indicates that investors quickly determined that the 'new' information was *not* material." *In re Allied Capital Corp. Sec. Litig.*, 2003 WL 1964184, at *6 (S.D.N.Y. Apr. 25, 2003) (finding no materiality where stock price recovered within a week); *see also SEC v. Butler*, 2005 WL 5902637, at *11–12 (W.D. Pa. April 18, 2005); *Mathews v. Centex Telemanagement, Inc.*, 1994 WL 269734, at *7 (N.D. Cal. June 8, 1994).[12] That factor is particularly relevant here because that drop coincided with inaccurate media reports that the vulnerabilities were unique to Intel and intractable. *See Hansen*, 527 F. Supp. 2d at 1161 (no materiality where statements leading to stock drop did not correct prior alleged misrepresentations).

II. Plaintiff Fails To Plead Facts Giving Rise to a Strong Inference of Scienter.

A. Plaintiff Does Not Plead Particularized Facts Showing That Defendants Believed Their Statements Were Materially False or Misleading, and the Most Obvious Inference Is Innocent.

To state a claim for securities fraud, the complaint must plead particularized facts giving rise to a strong inference of scienter—i.e., that the defendant acted with an intent to deceive, manipulate, or defraud. *Metzler*, 540 F.3d at 1061. A defendant must have acted with at least "deliberate recklessness" to be liable. *Zucco*, 552 F.3d at 991. A strong inference of scienter exists "'only if a reasonable person would deem the inference of scienter cogent and at least as compelling as any

[12] Another important consequence of the rapid and complete recovery of the stock price is that very few investors will be able to claim any damages in light of the PSLRA's 90-day bounceback provision, 15 U.S.C. § 78u-4(e)(1), which provides that any damages award "shall not exceed the difference between the purchase . . . price paid . . . by the plaintiff for the subject security and the mean trading price of that security during the 90-day period beginning on the date on which information correcting the misstatement or omission that is the basis for the action is disseminated to the market."

opposing inference one could draw from the facts alleged.'" *Id*. (quoting *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007)). Plaintiff must plead scienter as to each Defendant individually. *See Rudolph v. UTStarcom*, 560 F. Supp. 2d 880, 891 (N.D. Cal. 2008). To plead scienter as to a corporate defendant generally requires that it be adequately pleaded as to an individual responsible for the statement in question. *See Glazer Cap. Mgmt., LP v. Magistri*, 549 F.3d 736, 744–45 (9th Cir. 2008).

As discussed above, Plaintiff has pleaded no facts establishing that Intel's statements were false or misleading or that Intel has been materially adversely affected by the vulnerabilities. But even assuming Plaintiff had adequately pleaded falsity and materiality, the Consolidated Complaint offers no particularized facts supporting the requisite "strong" inference of scienter, in light of the overwhelming competing inference of innocence.

Most importantly, Intel's adherence to the Responsible Disclosure protocol supplied an obvious good reason not to disclose the Spectre and Meltdown vulnerabilities prematurely. The disclosure of new security vulnerabilities before remedies are deployed puts end users of Intel's products at risk. That is why the technology industry adheres to the Responsible Disclosure approach, and did so here. Many other companies—including Microsoft, Apple, Google, Amazon, Dell, AMD, and Arm—knew of Spectre and Meltdown during the putative class period, and none disclosed it publicly. Under these circumstances, no inference of fraud could be as strong as the obvious inference of innocence—that Intel followed the responsible, industry-wide approach to disclosure, which is designed to prevent harm to everyone, including Intel's customers and shareholders.

This case is controlled by *NVIDIA*, 768 F.3d 1046, in which the Ninth Circuit held that "delay[ing] disclosure while [a company] investigate[s] the cause of [a] chip defect[] and the extent of its liability" does not give rise to a strong inference of scienter. *Id.* at 1065. There, purchasers of NVIDIA chips privately advised NVIDIA of problems with its chips. *Id*. at 1049. NVIDIA assisted the customers in issuing software updates to address the problem. *Id*. at 1050. Ultimately, the customers determined a different root cause of the problem, which NVIDIA then investigated and confirmed, although it continued to contest its responsibility. *Id*. NVIDIA disclosed the issues to investors approximately a year after it was first advised of the problems; took a $196 million charge

to earnings; and saw its stock price fall by 31%. The Ninth Circuit concluded that "[t]he most compelling inference that we can reasonably draw is that NVIDIA was first investigating the root cause, and then the scope," of the problem, and that "[a]ny inference of scienter requires more than this." *Id*. at 1056. The court also found significant that "product flaws are very common in the semiconductor industry," and that NVIDIA had warned investors of that risk, which made any inference of scienter "not a cogent and compelling inference." *Id*. at 1065. The same conclusion applies to security vulnerabilities, which also are common and about which Intel had warned investors.

Moreover, the Consolidated Complaint pleads no facts showing that any Defendant believed that any of the statements listed by Plaintiff would mislead investors. This failure is fatal because a plaintiff must allege "more than simple conscious nondisclosure." *In re Canandaigua Sec. Litig*., 944 F. Supp. 1202, 1213 (S.D.N.Y. 1996). Plaintiff must plead not only that Defendants knew the facts, but also that they believed that they were misleading investors or were deliberately reckless. *Zucco*, 552 F.3d at 991; *Rigel*, 697 F.3d at 883. "[K]nowing about the existence of [problems] and knowing that one should report these [problems] to the public are two different things." *Colyer v. Acelrx Pharm., Inc.*, 2015 WL 7566809, at *13 (N.D. Cal. Nov. 25, 2015). For example, as the Supreme Court pointed out long ago, if a corporate official "mistakenly think[s] the [omitted] information . . . is not material," there is no scienter. *Dirks v. SEC*, 463 U.S. 646, 662–63 (1983).

The Consolidated Complaint fails under these standards. It makes no mention of any "specific contemporaneous statements or conditions" that contradict the statements made by the Defendants as of the time those statements were made. *Metzler*, 540 F.3d at 1066, 1071; *see also Dynavax*, 2018 WL 2554472, at *8 (granting motion to dismiss where scienter allegations not supported by "internal documents, confidential witness statements, or [relevant] correspondence"). That point is particularly apt here, where the great majority of allegedly misleading statements were advertisements posted long before the putative class period. Plaintiff offers no facts showing that anyone at Intel, much less the named individual Defendants, considered those statements to be misleading.

Nor does the Consolidated Complaint plead facts showing that Defendants believed the vulnerabilities—just two of many vulnerabilities Intel routinely encountered and remediated—were

material. Plaintiff has pleaded no facts sufficient to create a strong inference that anyone at Intel ever believed that these vulnerabilities would have a material financial impact on the company. Plaintiff cannot even make such a claim with the benefit of hindsight (unlike a typical securities case where materially negative events ultimately occurred). Thus, there is every reason to credit Intel's statements on January 3, 2018 and thereafter that it expected no material impact. Ex. 12. Intel was working with other companies to solve an industry-wide problem and believed that the solutions would work. Intel had disclosed many other security vulnerabilities (and solutions) before—and Plaintiff concedes that it planned to disclose Spectre and Meltdown, too, at the appropriate time. There is, therefore, no reason to think that Defendants acted with scienter in not disclosing the vulnerabilities earlier.

Again, *NVIDIA* is instructive. The court found significant that "Plaintiffs never allege that . . . anyone . . . at NVIDIA knew at that time . . . that NVIDIA's liability would exceed its normal reserve set aside for costs associated with product failures." 768 F.3d at 1059. Similarly, as discussed above, Plaintiff here fails to allege any facts showing that anyone at Intel believed Spectre and Meltdown were material issues. And unlike *NVIDIA*, where the problem eventually resulted in a $196 million charge, Plaintiff does not plead that Intel has sustained ***any*** financial impact.

"Problems and difficulties are the daily work of business people" and thus their existence "does not make a lie" out of everything a company says. *Ronconi v. Larkin*, 253 F.3d 423, 434 (9th Cir. 2001). There simply is no duty to disclose "every hitch or glitch . . . in 'real time.'" *City of Livonia Emps.' Ret. Sys. & Local 295/Local 851 v. Boeing Co.*, 711 F.3d 754, 759 (7th Cir. 2013). And it is no badge of scienter that a company declines to state publicly that "we have a problem . . . but we're working on [it] and we hope we can fix it . . . but we can't be sure, so stay tuned." *Id.* at 758. Yet that is precisely what Plaintiff's theory would have demanded that Intel tell the public.

B. Plaintiff's Trading Allegations Do Not Raise a Strong Inference of Scienter.

Plaintiff invokes the sale of Intel stock during the putative class period by a single insider, Defendant Krzanich, as evidence of scienter. This is insufficient as a matter of law. Although courts recognize that trading by insiders "'***may*** constitute circumstantial evidence of scienter,'" *Metzler*, 540 F.3d at 1066 (quoting *In re Silicon Graphics Inc. Sec. Litig.*, 183 F.3d 970, 986 (9th Cir.

1999), *superseded by statute on other grounds as stated in In re Quality Sys., Inc. Litig.*, 865 F.3d 1130, 1146 (9th Cir. 2017)) (emphasis added), "the significance that can be ascribed to an allegation of motive [such as insider trades] depends on the entirety of the complaint," *Tellabs*, 551 U.S. at 325. Courts in this circuit have dismissed many complaints despite allegations of significant insider sales. *See Silicon Graphics*, 183 F.3d at 987–88 (no strong inference of scienter where two insiders sold 43.6% and 75.3% of their shares); *Curry v. Yelp Inc.*, 875 F.3d 1219, 1226–27 (9th Cir. 2017) ($81.5 million in stock sales); *Metzler*, 540 F.3d at 1067 (two insiders sold $33 million in stock, including 100% of one defendant's stock); *In re Vantive Corp. Sec. Litig.*, 283 F.3d 1079, 1093–96 (9th Cir. 2002) (seven insiders sold $36 million in stock, including chairman who sold 74% of his shares), *abrogated on other grounds as recognized in South Ferry LP, No.2 v. Killinger*, 542 F.3d 776, 782–84 (9th Cir. 2008); *Ronconi*, 253 F.3d at 435–36 (eleven defendants traded, including seven who sold at least 69% of their shares and an eighth sold 98%); *In re Apple Comput. Sec. Litig.*, 886 F.2d 1109, 1117 (9th Cir. 1989) (insiders sold $84 million of stock); *Greenberg v. Cooper Cos., Inc.*, 2013 WL 100206, at *8–9 (N.D. Cal. Jan. 7, 2013). No inference of fraud arises from Mr. Krzanich's sales, for several reasons.

First, the theory that Mr. Krzanich's trading shows an intent to profit from the alleged fraud fails at the most basic level—he did not benefit from selling rather than holding. The inference of scienter "makes no sense when there is no benefit to a defendant in the sales," *Eng v. Edison Int'l*, 2016 WL 4793185, at *8 (S.D. Cal. Sept. 14, 2016), *appeal docketed*, No. 18-55496 (9th Cir. April 16, 2018)), and that is the case here. Mr. Krzanich's sales during the class period were at an average price of $44.19; the closing price of Intel stock on January 3, immediately ***after*** the public disclosure of the issue, was ***higher*** ($45.26), and even after the final alleged corrective disclosure on January 10, the low point was $42.44, only about 5% below Mr. Krzanich's average selling price. Ex. 14. Within a week, the price was once again above his average selling price of $44.19, and it hit $50 before the end of January. Ex. 14. The average price during the 90 days following the last allegedly corrective disclosure was $48.19, approximately 9% higher than Mr. Krzanich's average selling price. Ex. 14. In sum, Mr. Krzanich was financially disadvantaged by selling stock before, as opposed to after, the public disclosure of the vulnerabilities.

The Ninth Circuit has held repeatedly that when an insider sells "at about what the stock was worth after the bad news [became] public," the sales do not support an inference of scienter. *Ronconi*, 253 F.3d at 435 (affirming dismissal where insiders sold at $54 and stock then rose to $74 before dropping to $49 on disclosure). "When insiders miss the boat [as] dramatically" as Mr. Krzanich did here, their trading contributes nothing to the scienter analysis. *Id.*; *see also City of Dearborn Hts. Act 345 Police & Fire Ret. Sys. v. Align Tech., Inc.*, 856 F.3d 605, 621–22 (9th Cir. 2017) (affirming dismissal where insider sold at a price "even lower than the price he could have obtained had he waited until [the allegedly withheld information] was actually disclosed"). Mr. Krzanich's trading was not "calculated to maximize the personal benefit from undisclosed inside information," *Metzler*, 540 F.3d at 1066–67, as the Ninth Circuit requires for any inference of fraud to arise.

Second, any inference of fraud from Mr. Krzanich's trading is undermined by the fact that Plaintiff does not allege that Defendant Swan, Intel's CFO (and now interim CEO), who Plaintiff alleges also was involved in the supposed fraud (CC ¶ 99), sold any shares of Intel stock during the class period. Nor does Plaintiff allege any unusual or suspicious trading by Defendant Shenoy. "One insider's well timed sales do not support the 'strong inference' required by the [PSLRA] where the rest of the equally knowledgeable insiders act in a way inconsistent with the inference that the favorable characterizations of the company's affairs were known to be false when made." *Ronconi*, 253 F.3d at 436 (footnote omitted); *see also Dynavax*, 2018 WL 2554472, at *9 (that two individual defendants purchased stock during the class period "undermin[es] an inference of scienter").

Third, Intel itself bought back millions of its own shares for more than a billion dollars after the date on which Plaintiff alleges Intel learned of the security vulnerabilities. Ex. 18. This conduct "rebuts a finding of scienter" because "it is illogical that [the company] would have been repurchasing its shares had it been aware of facts that would indicate the price would fall." *Cisco*, 2013 WL 1402788, at *8; *see also In re Tibco Software, Inc. Sec. Litig.*, 2006 WL 1469654, at *21 (N.D. Cal. May 25, 2006).

Finally, even if the Court were inclined to draw some inference of scienter from Mr. Krzanich's sales, it would be less cogent than the more obvious innocent inference—Intel did not believe the vulnerabilities were material and adhered to the Responsible Disclosure protocol in

determining when and how to disclose. *See Silicon Graphics*, 183 F.3d at 987–88 (even though two insiders' sales were "somewhat suspicious," no strong inference of scienter under all the circumstances).

C. The Other Alleged Indicia of Scienter Do Not Give Rise to a Strong Inference.

Plaintiff throws in an assortment of other allegations to support a strong inference of scienter. None does so. Several of Plaintiff's assertions go only to show that Defendants were aware of Spectre and Meltdown during the class period. *See, e.g.*, CC ¶¶ 170–74, 177. But "knowing about the existence of [problems] and knowing that one should report these [problems] to the public are two different things." *Colyer*, 2015 WL 7566809, at *13. As discussed above, Plaintiff fails to show either that Defendants had a duty to disclose or that they believed that investors would be misled.

The Consolidated Complaint also refers to four alleged former employees of Intel, but the information attributed to them has no capacity to show scienter. None of the former employees appears to have any personal knowledge concerning Spectre and Meltdown. Two of them no longer worked at Intel when the issues arose. *See* CC ¶¶ 72 (employment ended in 2016), 74 (employment ended January 2017). The best these four witnesses can do is to describe Intel's alleged "standard process" or what they believe "would" have happened in response to the security vulnerabilities. CC ¶¶ 72–75, 112. These conditional statements do not demonstrate personal knowledge on the part of the witnesses. *See, e.g.*, *NVIDIA*, 768 F.3d at 1064; *In re Nimble Storage Sec. Litig.*, 2017 WL 4355570, at *5 (N.D. Cal. Oct. 2, 2017); *Greenberg*, 2013 WL 100206, at *8. Moreover, even if the statements were credited, none of them is relevant to scienter because none shows that any Defendant believed that investors were being misled. *See Zucco*, 552 F.3d at 995. At most, these witnesses' statements might indicate that Defendants were aware of Spectre and Meltdown, but, as described above, that is not sufficient to show scienter.

Plaintiff also faults Intel for not notifying US-CERT of Spectre and Meltdown earlier than it did.[13] CC ¶ 175. But even if the US-CERT guidelines for reporting to the federal government applied

[13] US-CERT is a separate entity from CERT/CC. *See* CC ¶¶ 67–68 (distinguishing US-CERT and CERT/CC).

here (and they did not[14]), Intel's compliance or non-compliance with them has no connection to whether it intended to mislead investors.

Finally, Plaintiff contends that the "suspicious timing and circumstances" of Mr. Krzanich's resignation in June 2018 support an inference of scienter. CC ¶ 176. An employee's resignation supports an inference of scienter only when "the resignation at issue was uncharacteristic when compared to the defendant's typical hiring and termination patterns or was accompanied by suspicious circumstances." *Zucco*, 552 F.3d at 1002. Otherwise, "the inference that the defendant corporation forced certain employees to resign because of its knowledge of the employee's role in the fraudulent representations will never be as cogent or as compelling as the inference that the employees resigned or were terminated for unrelated personal or business reasons." *Id.* As the Consolidated Complaint acknowledges, Intel has stated that the reason for Mr. Krzanich's departure—five months after Spectre and Meltdown came to light—was a consensual relationship with another Intel employee, which violated Intel's policies. CC ¶ 176. Plaintiff alleges no facts that could connect Mr. Krzanich's resignation to the security vulnerabilities disclosed months earlier. Moreover, the fact that Defendant Swan was appointed by Intel's Board of Directors as interim CEO contemporaneously with Mr. Krzanich's resignation fatally undermines any inference of scienter, as does Defendant Shenoy's continued tenure as an Executive Vice President ("EVP"). *See Align*, 856 F.3d at 622; *NVIDIA*, 768 F.3d at 1062–63.

III. The Control-Person Claim Fails To State a Claim.

Control-person liability under Section 20(a) requires a predicate violation by the allegedly controlled person. Because no direct claim under Section 10(b) has been stated here, there is no viable claim for control-person liability. *See, e.g.*, *Zucco*, 552 F.3d at 990.[15] Moreover, Plaintiff's control

[14] Although Plaintiff does not provide a citation for the guidelines it quotes, it apparently is referring to the US-CERT Federal Incident Notification Guidelines (Ex. 19). Those guidelines, however, apply only to federal agencies; adherence by private companies is voluntary. In addition, Spectre and Meltdown did not constitute an "incident" as defined in the US-CERT guidelines, which requires an "imminent" threat to, *inter alia*, information systems or security procedures. Ex. 19.

[15] For the reasons discussed above, the allegations concerning statements attributed to Mr. Krzanich (CC ¶ 155), Mr. Swan (CC ¶ 162), and Mr. Shenoy (CC ¶¶ 88, 159–60) fail to state a viable claim for the same reasons as the allegations concerning statements attributed only to Intel.

allegations with respect to Mr. Shenoy are perfunctory and fail to allege that he was a controlling person. Plaintiff alleges only that Mr. Shenoy was, during the purported class period, Intel's EVP and General Manager of the Data Center Group; was a long-time Intel employee; was knowledgeable about the activities of his group; and played a role in communicating with Intel's customers about remediation efforts for Spectre and Meltdown. CC ¶ 21. These allegations are insufficient to show that Mr. Shenoy exercised "'a significant degree of day-to-day operational control, amounting to the power to dictate another party's conduct or operations.'" *In re Impac Mortg. Holdings, Inc. Sec. Litig.*, 554 F. Supp. 2d 1083, 1101 n.12 (C.D. Cal. 2008) (quoting *In re McKesson HBOC, Inc. Sec. Litig.*, 126 F. Supp. 2d 1248, 1277 (N.D. Cal. 2000)).

In addition, Mr. Shenoy's position at Intel is insufficiently senior for him to qualify as a controlling person. *See, e.g.*, *In re Int'l Rectifier Corp. Sec. Litig.*, 2008 WL 4555794, at *22 (C.D. Cal. May 23, 2008) (dismissing control person claims against company's Executive Vice President because his position "d[id] not establish that he had control."); *Middlesex Ret. Sys. v. Quest Software Inc.*, 527 F. Supp. 2d 1164, 1194 (C.D. Cal. 2007) (rejecting control person liability claim against vice president); *In re Gap Stores Sec. Litig.*, 457 F. Supp. 1135, 1137, 1143 (N.D. Cal. 1978) (rejecting control person liability for corporate vice president where defendant was a "lesser member" of the corporation's management and "not able to . . . control the decisions of the executive officers or the corporation").

Finally, bare legal conclusions and boilerplate allegations of "control" are insufficient to state a claim under Section 20(a). *See City of Westland Police & Fire Ret. Sys. v. Sonic Sols.*, 2009 WL 942182, at *11 (N.D. Cal. Apr. 6, 2009). In particular, Plaintiff pleads no specific facts, as opposed to boilerplate assertions, showing that Mr. Shenoy had any involvement in any allegedly misleading statements (other than his own). *See, e.g.*, *Paracor Fin., Inc. v. Gen. Elec. Capital Corp.*, 96 F.3d 1151, 1163–64 (9th Cir. 1996) (CEO was not a control person where he did not have control over offering materials containing alleged misstatements); *Special Situations Fund III QP, L.P. v. Brar*, 2015 WL 1393539, at *10 (N.D. Cal. Mar. 26, 2015) (dismissing allegation that defendants "had the power, influence and authority to cause, and did cause, directly or indirectly, others to engage in the wrongful conduct complained of herein, including the content and dissemination of the various

statements which Plaintiffs contend are false and misleading," among others, as "boilerplate allegations that courts have typically rejected" (internal quotation marks omitted). Thus, even if any of Plaintiff's claims as to statements made by persons other than Mr. Shenoy were viable (which they are not), the Section 20(a) claim against him must be dismissed.

CONCLUSION

For the foregoing reasons, the Court should dismiss Plaintiff's Consolidated Complaint with prejudice. Plaintiff already has amended its complaint once, and denial of leave to amend is appropriate where further amendment would be futile. *See, e.g.*, *Salameh v. Tarsadia Hotel*, 726 F.3d 1124, 1133 (9th Cir. 2013); *Wanca v. Super Micro Comput., Inc.*, 2018 WL 3145649, at *9 (N.D. Cal. June 27, 2018), *appeal docketed*, No. 18-16391 (9th Cir. July 25, 2018). That is the case here because Defendants' statements are not actionable as a matter of law and Intel has suffered no material financial consequences.

Dated: August 29, 2018

Respectfully submitted,

By: /s/ STEVEN M. FARINA

STEVEN M. FARINA
GEORGE A. BORDEN
MARGARET A. KEELEY
COLETTE T. CONNOR
XIAO WANG
WILLIAMS & CONNOLLY LLP
725 Twelfth Street, N.W.
Washington, DC 20005
Tel: (202) 434-5000
Fax: (202) 434-5029
sfarina@wc.com
gborden@wc.com
mkeeley@wc.com
cconnor@wc.com
xwang@wc.com

JOHN W. SPIEGEL
(State Bar No. 78935)
ROBERT L. DELL ANGELO
(State Bar No. 160409)
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, 50th Floor
Los Angeles, CA 90071
Tel: (213) 683-9100

Fax: (213) 683-5141
john.spiegel@mto.com
robert.dellangelo@mto.com

Attorneys for Defendants Intel Corporation, Brian M. Krzanich, Robert H. Swan, and Navin Shenoy

Pursuant to Civil Local Rule 5.1(i)(3), I, Robert L. Dell Angelo, hereby attest that concurrence in the filing of this document has been obtained from the above signatory.